

Docket No. AUS920010449US1

CLAIMS:

What is claimed is:

1. A method in a data processing system for
5 automatically configuring IP security tunnels, said
method comprising the steps of:
 establishing a security policy specification format
capable of being utilized by a plurality of different
operating systems and a plurality of different machine
10 types; and
 defining a configuration of an IP security tunnel
utilizing said security policy specification format.
2. The method according to claim 1, further comprising
15 the step of establishing said security policy
specification format as a DTD file.
3. The method according to claim 2, further comprising
the step of including a plurality of different elements
20 in said DTD file, each of said plurality of different
elements being utilized to configure an IP security
tunnel.
4. The method according to claim 1, further comprising
25 the steps of:
 generating an XML file utilizing a plurality of said
plurality of tags included within said DTD file; and
 processing said XML file to automatically configure
an IP security tunnel.

Docket No. AUS920010449US1

5. The method according to claim 1, further comprising the step of including a root element in said security policy specification format.

5 6. The method according to claim 1, further comprising the step of establishing a protection element in said security policy specification format, said protection element including a listing of IKE transforms.

10 7. The method according to claim 1, further comprising the step of establishing a transform element in said security policy specification format.

15 8. The method according to claim 1, further comprising the step of establishing a group element in said security policy specification format.

20 9. The method according to claim 1, further comprising the step of establishing an identification element in said security policy specification format.

10. The method according to claim 1, further comprising the step of establishing a tunnel element in said security policy specification format.

25 11. The method according to claim 1, further comprising the step of establishing a root element, a protection element, a transform element, a group element, an identification element, a tunnel element, a local/remote
30 identify element, an ID type element, an ID definition element, a pre-shared key element, an IPsec proposal element, an IPsec ESP protocol element, an IPsec

Docket No. AUS920010449US1

authentication header element, and an IPsec protection element in said security policy specification format.

12. The method according to claim 1, further comprising
5 the step of automatically configuring an IP security tunnel utilizing said security policy specification format.

13. The method according to claim 1, further comprising
10 the step of comparing a first IP security tunnel to a second IP security tunnel utilizing a first security policy specification format that is associated with said first IP security tunnel and a second security policy specification format that is associated with a second IP
15 security tunnel.

14. A computer program product for defining a configuration of IP security tunnels, comprising:
instruction means for establishing a security policy
20 specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types; and

instruction means for automatically configuring an IP security tunnel utilizing said security policy
25 specification format.

15. The product according to claim 14, further comprising instruction means for establishing said security policy specification format as a DTD file.

30

16. The product according to claim 15, further comprising instruction means for including a plurality of

Docket No. AUS920010449US1

different elements in said DTD file, each of said plurality of different elements being utilized to configure an IP security tunnel.

- 5 17. The product according to claim 14, further comprising:

instruction means for generating an XML file utilizing a plurality of said plurality of tags included within said DTD file; and

- 10 instruction means for processing said XML file to automatically configure an IP security tunnel.

- 15 18. The product according to claim 14, further comprising instruction means for including a root element in said security policy specification format.

19. The product according to claim 14, further comprising instruction means for establishing a protection element in said security policy specification
20 format, said protection element including a listing of IKE transforms.

20. The product according to claim 14, further comprising instruction means for establishing a transform
25 element in said security policy specification format.

21. The product according to claim 14, further comprising instruction means for establishing a group element in said security policy specification format.

30

22. The product according to claim 14, further comprising instruction means for establishing an

Docket No. AUS920010449US1

identification element in said security policy specification format.

23. The product according to claim 14, further
5 comprising instruction means for establishing a tunnel element in said security policy specification format.

24. The product according to claim 14, further
10 comprising instruction means for establishing a root element, a protection element, a transform element, a group element, an identification element, a tunnel element, a local/remote identify element, an ID type element, an ID definition element, a pre-shared key element, an IPsec proposal element, an IPsec ESP protocol
15 element, an IPsec authentication header element, and an IPsec protection element in said security policy specification format.

25. The product according to claim 14, further
20 comprising instruction means for automatically configuring an IP security tunnel utilizing said security policy specification format.

26. The product according to claim 14, further
25 comprising instruction means for comparing a first IP security tunnel to a second IP security tunnel utilizing a first security policy specification format that is associated with said first IP security tunnel and a second security policy specification format that is
30 associated with a second IP security tunnel.

27. A data processing system for defining a configuration of IP security tunnels, comprising:

5 systems and a plurality of different machine types; and

10 28. The system according to claim 27, further comprising
said security policy specification format being
established as a DTD file.

29. The system according to claim 28, further comprising
15 a plurality of different elements being included in said
DTD file, each of said plurality of different elements
being utilized to configure an IP security tunnel.

30. The system according to claim 27, further
20 comprising:
an XML file being generated utilizing a plurality of
said plurality of tags included within said DTD file; and
said system for processing said XML file to
automatically configure an IP security tunnel.

31. The system according to claim 27, further comprising a root element being included in said security policy specification format.

30 32. The system according to claim 27, further comprising
a protection element being included in said security

Docket No. AUS920010449US1

policy specification format, said protection element including a listing of IKE transforms.

33. The system according to claim 27, further comprising
5 a transform element being included in said security policy specification format.

34. The system according to claim 27, further comprising
10 a group element being included in said security policy specification format.

35. The system according to claim 27, further comprising
15 an identification element being included in said security policy specification format.

36. The system according to claim 27, further comprising
a tunnel element being included in said security policy specification format.

20 37. The system according to claim 27, further comprising a root element, a protection element, a transform element, a group element, an identification element, a tunnel element, a local/remote identify element, an ID type element, an ID definition element, a pre-shared key
25 element, an IPsec proposal element, an IPsec ESP protocol element, an IPsec authentication header element, and an IPsec protection element being included in said security policy specification format.

30 38. The system according to claim 27, further comprising said system for automatically configuring an IP security

Docket No. AUS920010449US1

tunnel utilizing said security policy specification
format.

39. The system according to claim 27, further comprising
5 said system for comparing a first IP security tunnel to a
second IP security tunnel utilizing a first security
policy specification format that is associated with said
first IP security tunnel and a second security policy
specification format that is associated with a second IP
10 security tunnel.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50